REMARKS

Upon entry of this amendment, Claims 15-47 will be pending in this application. In view of the foregoing amendments and the following remarks, applicant respectfully requests consideration of the new Claims.

New Claims 15-47 are not anticipated or made obvious by, and further differentiate the claimed invention over the prior art of record. Elements that contribute to the Claims' novelty include, but are not limited to, the following.

Claim 15 recites the delivery of the encrypt/decrypt engine via a web page, encryption independent from the identity of the client. Ross requires dependence on the identity of the client.

Claim 17 recites delivery of stored data responsive to completion of a processing step.

Claim 18 recites storage of encrypted data followed by delivery of the stored data responsive to a request from either the original client or another client.

Claim 19 recites lower limits on the number of times a key must be transmitted.

Claim 22 recites an encrypt/decrypt engine configured to operated independently of the identity of the client.

Claim 23 recites decryption and re-encryption of the data using a key of the server.

Claim 24 recites encryption of data for delivery responsive to the completion of a processing step. The encryption using the shared key or another shared key. Delivery may be to the client or another client.

Claim 25 is similar to Claim 24 except that operation is responsive to a request for the data.

Claims 25 and 26 include two possibilities for the source of a request for data.

Claim 28 recites the restriction of storage, of all data entered by the user on the client, to storage in encrypted form. Claim 28 also recites use of a key entered by the user for encryption.

Claim 29 recites use of a symmetric key.

Claim 31 is a method claim reciting use of a web page to deliver the encrypt/decrypt engine and reciting use of a shared key entered by a user.

Claims 32-36 include various methods of processing the data receive at the server.

Claims 37-41 recites a computer-readable medium comprising program instructions. The program instructions may execute methods of the invention possibly using the systems of the invention.

Claim 42 is a method claim including encryption of data independently of an identity of the client using a shared key entered by a user.

Claim 43-46 include further details of the step of processing data decrypted at the server.

Conclusion

The Applicant respectfully request a Notice of Allowability. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Dated: April 2, 2002

By: 

Steven M. Colby, Ph.D. Reg. No. 50,250
Carr & Ferrell, LLP
2225 E. Bayshore Road, Suite 200
Palo Alto, CA 94303
Tel: (650) 812-3424
Fax: (650) 812-3444
e-mail: scolby@carr-ferrell.com

Appendix showing changes to the Specification.

On page 6 starting at line 14:

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private keys with anyone else.

On page 8 starting at line 6:

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module ~~404~~ 406 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.